

SchARR Certified Data Deletion Procedure

This version (v2) Approved at IG Committee Meeting 2022.01.24

This process should be read in conjunction with the document "[Technical description of what happens when files are deleted](#)" that describes what happens when a file is deleted.


If a data deletion certificate signed by the IG lead / manager is required, the files containing the data should not be deleted by the user.

SchARR process for requesting certified data deletion:

For data held in a project folder on the X drive


Project team:	Contact SchARR DS to say that there are data on the X drive that need deleting for which a deletion certificate is required. Give SchARR DS the project details (name of project and name of X drive folder) and indicate whether all contents of the folder or only certain files need deleting.
Project team:	Delete all contents
SchARR DS:	Create a new control folder in the project shared area ”.
Project team:	Copy (not move) all files that are to be retained into the new control folder. Delete all contents of original folder
SchARR DS:	Remove all project team access to the original control folder and request deletion from Storage & Server.
SchARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by NHS digital).
IG lead / IG manager:	complete and sign the NHS Digital Certificate of Data Destruction and send to project team; include the details of the data to be destroyed, as outlined in the data sharing agreement (DSA).
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send certificate to NHS Digital

For data held in a VM filestore where SchARR-DS have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include NHS Digital data, and if it includes derived data this must have been confirmed as such by NHS digital according to their template). Anything left in the VM filestore will be deleted.
Project team:	Shut down VM. Start menu >  > Shut down
Project team:	Contact SchARR DS to say that there are data in a VM filestore that need deleting for which a deletion certificate is required. Give SchARR DS the project details (name of project and name of the VM).
SchARR DS:	Contact IT Services to delete VM and VM filestore.
SchARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by NHS digital).
IG lead / IG manager:	complete and sign the NHS Digital Certificate of Data Destruction and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send certificate to NHS Digital.

For data held in a VM filestore where SchARR-DS do not have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include NHS Digital data, and if it includes derived data this must have been confirmed as such by NHS digital according to their template). Anything left in the VM filestore will be deleted.
---------------	--

Project team:	Shut down VM. Start menu >  > Shut down
Project team:	Contact ScHARR DS to say that there are data in a VM filestore that need deleting for which a deletion certificate is required. Give ScHARR DS the project details (name of project and name of the VM).
ScHARR DS:	Contact IT Services to delete VM and VM filestore.
ScHARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by NHS digital).
IG lead / IG manager:	complete and sign the NHS Digital Certificate of Data Destruction and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send certificate to NHS Digital

For data held in the Data Safe Haven

Project team:	Contact the Data Safe Haven team regarding data destruction
DSH team:	To ensure data destruction is carried out and documented in accordance with the documented process maintained by the DSH team

Version	Effective Date	Summary of changes
1.0	08-May-2020	n/a first version
2.0	24-Jan-2022	Updated to include the DSH. Process to delete X drive data updated to protect the data from recovery